

5 FAH-2 H-820 SECURITY SAFEGUARDS

(CT:TEL-20; 07-25-2007)
(Office of Origin: (A/LM/AQM/IT/COM))

5 FAH-2 H-821 SECURE HANDLING

(CT:TEL-20; 07-25-2007)
(Uniform all agencies)

- a. *Secure handling* applies to selecting the shipping method most appropriate for the type of material, area where it will be used, and threat level of the post.
- b. *Secure handling procedures are outlined in 12 FAH-6*, OSPB Security Standards and Policy Handbook, and *5 FAH-6*, Communications Security Handbook.
- c. If it is suspected that equipment is compromised, contact the *Regional Security Officer (RSO)* who may elect to obtain further guidance from *the Office of Computer Security (DS/SI/CS) and the Office of Information Technology Infrastructure's Technical Security and Safeguard Division (IRM/OPS/ITI/TSS)*, for disposition of the equipment. *Technical Security and Safeguards (TSS) Field Surety Engineers (FSE)* maintain the life cycle security for equipment at post that have TSS applied security and safeguards. TSS/FSE must be notified if any of that equipment is suspected of compromise.

5 FAH-2 H-822 ACCESS CONTROL

(CT:TEL-20; 07-25-2007)
(Uniform all agencies)

- a. The RSO at post is responsible for restricting access to classified information systems to individuals cleared at the highest classification level of information processed on the equipment (*12 FAM 600*).
- b. Access to the *Information Program Center (IPC)* is restricted to those individuals authorized by the *Chief of Missions (COM)* as prescribed by 5 FAH-6, which is a classified Communications Security Handbook. Any

other individuals who require access to the IPC must be escorted. IPC must keep a written record of all authorized visitors as prescribed by 5 FAH-6, Communications Security Handbook.

5 FAH-2 H-823 THROUGH H-829 UNASSIGNED